Code Red (virus)

Code Red was a computer worm observed on the Internet on July 15, 2001.

It attacked computers running Microsoft's IIS web server. It was the first large scale, mixed threat attack to successfully target enterprise networks.

The Code Red worm was first discovered and researched by eEye Digital Security employees Marc Maiffret and Ryan Permeh when it exploited a vulnerability discovered by Riley Hassell. They named it "Code Red" because Code Red Mountain Dew was what they were drinking at the time.[

Although the worm had been released on July 13, the largest group of infected computers was seen on July 19, 2001. On this day, the number of infected hosts reached 359,000.

- ### How does Code Red work?

Code Red works its way into a target computer and uses it as a base to mount attacks on official websites. It is time sensitive, carrying out different actions depending on the date of the month.

During the first 19 days of the month, a Code Red infected computer will scan the internet, targeting and infecting other vulnerable computers.

From days 20 to 27, it will launch so-called "denial of service" attacks on one of several US government websites, by flooding a website with requests for access until they fail under the weight of internet traffic. After the 27th day, the worm remains in the computer's memory but is otherwise inactive.

The FBI yesterday issued an urgent warning to businesses urging them to make sure they are protected against the worm. It feared that Code Red would reactivate in computers, where it had been lying dormant, at 1am BST today as it returns to day one of its monthly cycle, and begins infecting new machines, disrupting the internet and potentially bringing it to a grinding halt.

- **Did that happen ?**

No. It appears that computer users have heeded the FBI's warnings and installed the necessary security patch to stop the worm.

The FBI said today that the internet is running normally despite the threat, but insisted that the effect of the worm might not be felt for several days.

However some computer experts claim that the FBI exaggerated the risk in the first place.

Graham Cluley, of Sophos Anti-Virus, said: "It's all been a bit of a damp squib so far.

"It looks like the soothsayers are the guys with egg on their faces this morning."

Tech news site the Register and virus hoax information site Vmyths both argue that the flood of warning emails, calls to antivirus support lines and general level of hysteria can cause more damage to the internet than the worm itself.

- **Who is behind the Code Red worm?**

  The origin of the attack is unclear. The FBI are attempting to track down the worm's author but their search has so far proved fruitless. The worm caused affected web server computers to deface the sites they operated, displaying a message that reads: "HELLO! Welcome to http://www.worm.com! Hacked by Chinese", sparking rumours that the attack was launched from China. However most experts believe that the message may be an attempt to create a diversion away from the worm's real author, rather than a true indication of Code Red's origins.

- ## Useful links

  Code Red worm profile - Trend Micro Virus Encyclopaedia
  Step-by-step instructions for eliminating the Code Red worm vulnerability - Digital Island
  Here comes the Code Red hysteria
  Information on "Code Red" IIS worm
  Microsoft security bulletin offering patch for Code Red
  CodeRed Scanner - eEye Digital Security
  How to recover your system following an attack by Code Red - Cert
  Things to remember when virus hysteria strikes - Vmyths.com
  Here comes the Code Red hysteria - Vmyths.com
  Code Red Tribulation is nigh, Steve Gibson warns - the Register
  30.07.2001, comment: Vigilance first, last and always - CNET

- ## External links

- Code Red II analysis, Steve Friedl's Unixwiz.net, last update 22 August 2001
- CAIDA Analysis of Code-Red, Cooperative Association for Internet Data Analysis (CAIDA) at the San Diego Supercomputer Center (SDSC), updated November 2008
- Animation showing the spread of the Code Red worm on 19 July 2001, by Jeff Brown, UCSD, and David Moore, CAIDA at SDSC

- ## Exploited vulnerability :

The worm showed a vulnerability in the growing software distributed with IIS, described in Microsoft Security Bulletin MS01-033, for which a patch had been available a month earlier.

The worm spread itself using a common type of vulnerability known as a buffer overflow. It did this by using a long string of the repeated letter 'N' to overflow a buffer, allowing the worm to execute arbitrary code and infect the machine with the worm. Kenneth D.

Eichman was the first to discover how to block it, and was invited to the White House for his discovery .

Masood Ghanim .

Questions and Answers about the virus code red

1) How many computers did Code Red infect ?

Code Red infected between 1 and 2 million **computers** and resulted in an estimated $2.75 billion in clean-up costs and lost productivity. This is out of a possible 6 million, as that is the number of IIS servers in existence at the time.
It **was** the most costly malware of 2001.

2) How did the Code Red infect computers ?

Code Red (**computer** worm) **Code Red** was a **computer** worm observed on the Internet on July 15, 2001. It attacked **computers** running Microsoft's IIS web server. ... They named it "**Code Red**" because **Code Red** Mountain Dew was what they **were** drinking at the time.

3) What did the Code Red and Code Red II viruses do?

The **Code Red and Code Red II** worms popped up in the summer of 2001.
The original **Code Red** worm initiated a distributed denial of service (DDoS) attack on the White House. That means all the computers infected with **Code Red** tried to contact the Web servers at the White House at the same time, overloading the machines.

4) What type of virus is code red?

Code Red was a **computer worm** that appeared in the summer of 2001 and attacked computers running Microsoft's **Internet Information Services** (**IIS**) web server .

5) What does the Code Red virus do?

Code Red (computer worm) **Code Red** was a computer worm observed on the Internet on July 15, 2001. It attacked computers running Microsoft's IIS web server. It was the first large scale, mixed threat attack to successfully target enterprise networks.

6) What is the most dangerous computer virus?

ILOVEYOU

1. ILOVEYOU is considered one of the **most** virulent **computer virus** ever created.
   It managed to wreck havoc on **computer** systems all over the world with around $10 billion worth of damages.

7) How did Code Red spread?

The worm spreads by probing random IP addresses and infecting all hosts vulnerable to the IIS exploit. As noted by others, there are at least two variants of the worm: one that used a fixed, static seed for its random number generator, and another that used a random seed.

8) What is the Code Red?

"**Code Red**" and "**Code** Blue" are both terms that are often used to refer to a cardiopulmonary arrest, but other types of emergencies (for example bomb threats, terrorist activity, child abductions, or mass casualties) may be given "**Code**" designations too.

9) Who created the Code Red worm?

Jeff Brown
Animations. To help us visualize the initial spread of **Code-Red** version 2, Jeff Brown **created** an animation of the geographic spread of the **worm** in five minute intervals between midnight UTC on July 19, 2001 and midnight UTC on July 20, 2001

10) When was Code Red invented?

They named it "Code Red" because Code Red Mountain Dew was what they were drinking at the time. Although the worm had been released on July 13, the largest group of infected computers was seen on **July 19, 2001**. On this day, the number of infected hosts reached 359,000.

...

Code Red (computer worm)

Common name	**Code Red**
Isolation	July 15, 2001

11) What is Code Red in cyber security?

Code Red was a **computer** worm observed on the Internet on July 15, 2001. It attacked computers running Microsoft's IIS web server. It was the first large scale, mixed threat **attack** to successfully target enterprise networks. ... They named it "**Code Red**" because **Code Red** Mountain Dew was what they were drinking at the time.

12) Is Code Red An antivirus software?

Code Red, as it was later named, targeted vulnerable IP addresses, and attacked those using Microsoft Windows 2000 or NT. Because Code Red is a file-less worm that exists in the system memory, anti-malware and scanning tools at the time weren't equipped to stop or remove it.

Masood Ghanim .